Session 309

Security: Kerberos

Thomas Weyer
Network & Communications Technology Manager

Agenda

- Overview of Kerberos
  - What it is
  - What is Apple doing with Kerberos
- Technical
  - How it works
  - Components overview
  - How to add Kerberos to your application
- Q&A

Audience Poll

What Kerberos Is

- A secure network authentication system
  - Authentication vs. Authorization
- Proves who you are
- Uses a trusted third party model security model

Who Uses Kerberos

- Government
- Large corporations
- Higher education
- Every Windows 2000 installation

Why Do They Use It?

- Mutual authentication
- Single sign on
- Factor security problem (Authentication vs. Authorization)
- Consistent with centralized Authentication goals
- Highly extensible/interfaceable
  - RADIUS, PAM, etc

Why Do They Use It?

- Inherently more secure than any other encrypted password exchange
- Ubiquitous
  - Mac, Win, Solaris, Mac OS X, Linux, HP-UX, AIX…
- Time tested
  - Developed in 1980's as part of Project Athena
- Source freely available

Apple and Kerberos

- Importance to our market(s)
- Press Release last year
- Mac Manager supports Kerberos
- Mac OS X and Kerberos

Kerberos for Macintosh

Marshall Vale
Project Manager: Macintosh and Kerberos Development
Massachusetts Institute of Technology

Kerberos Terms

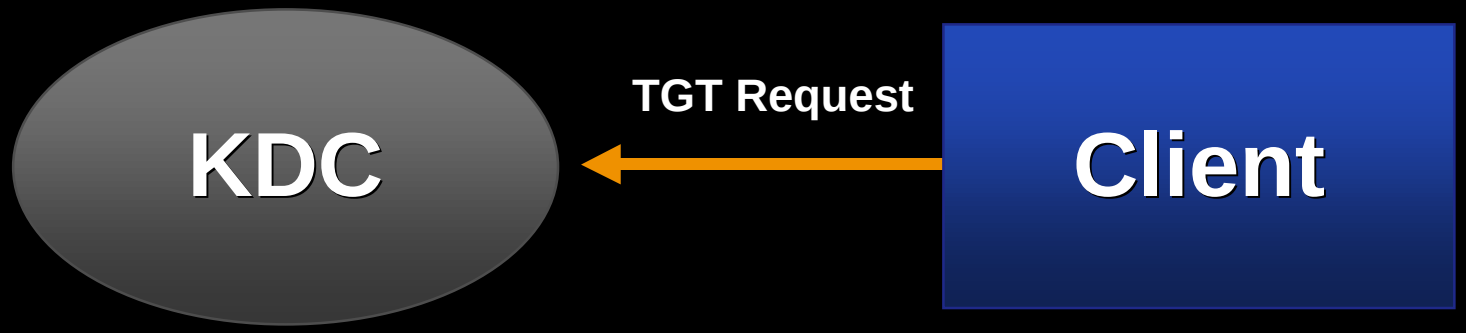
- Realm
  - The administrative unit protected by a KDC
- Ticket
  - An authentication token
- Ticket-granting ticket (TGT)
  - An initial ticket that grants permission to get service tickets
- Service ticket
  - A ticket that authenticates the user to a particular service (e.g., ftp, mail, telnet)

Ticket Granting Ticket (TGT)

- Also called “initial ticket” because it’s the first ticket a client gets
- Proves that the client is allowed to get tickets for other services
- Acts as a substitute for password
- Only valid for a limited period of time (expires)

Getting a TGT

- Client asks KDC for TGT

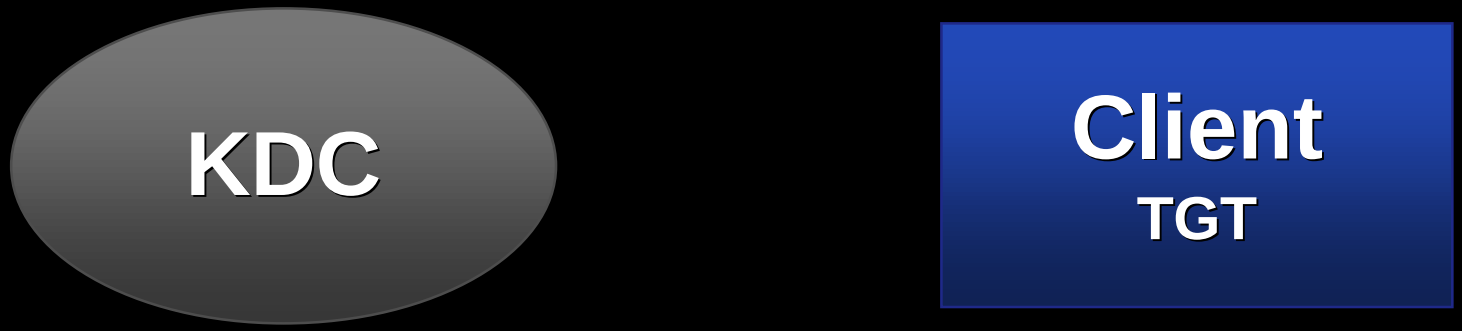


Getting a TGT

- KDC returns a TGT and session key to a client encrypted with client's key

Getting a TGT

- Client uses client's key (one-way hash of password) to extract TGT

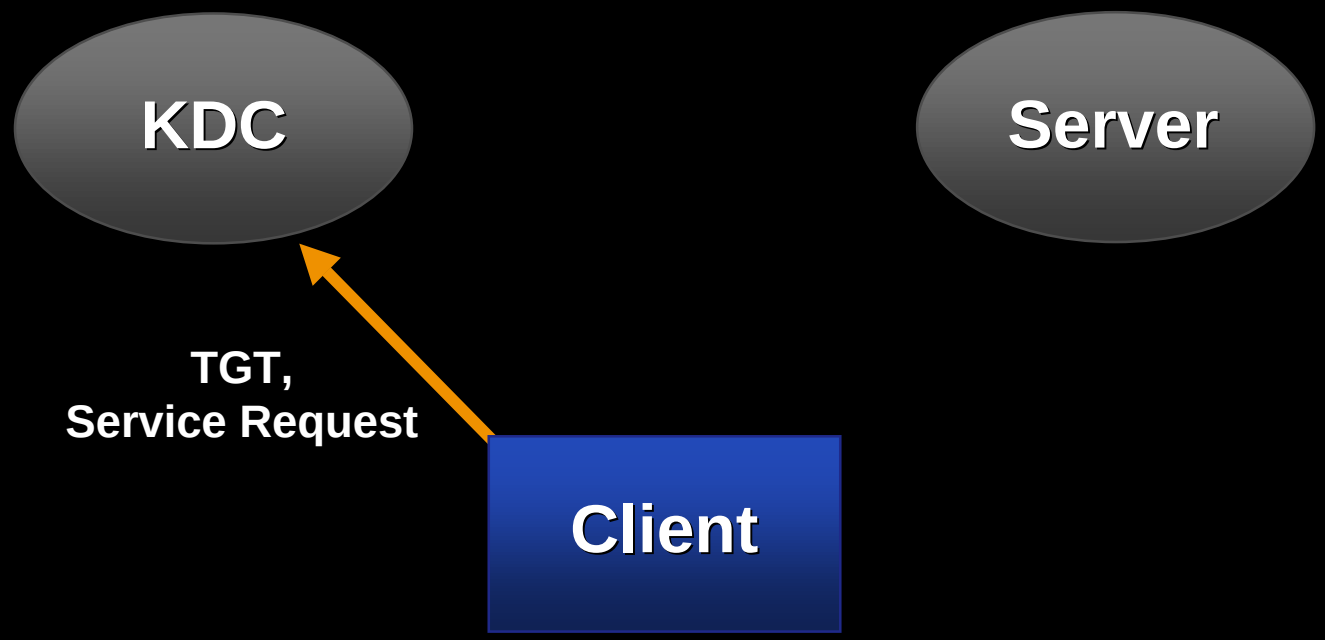


Service Ticket

- Ticket used by client to get access to particular service or server (e.g., ftp, mail, telnet)
- Contains a session key which is shared between the client and server that they can use to encrypt data exchanges
- Also expires

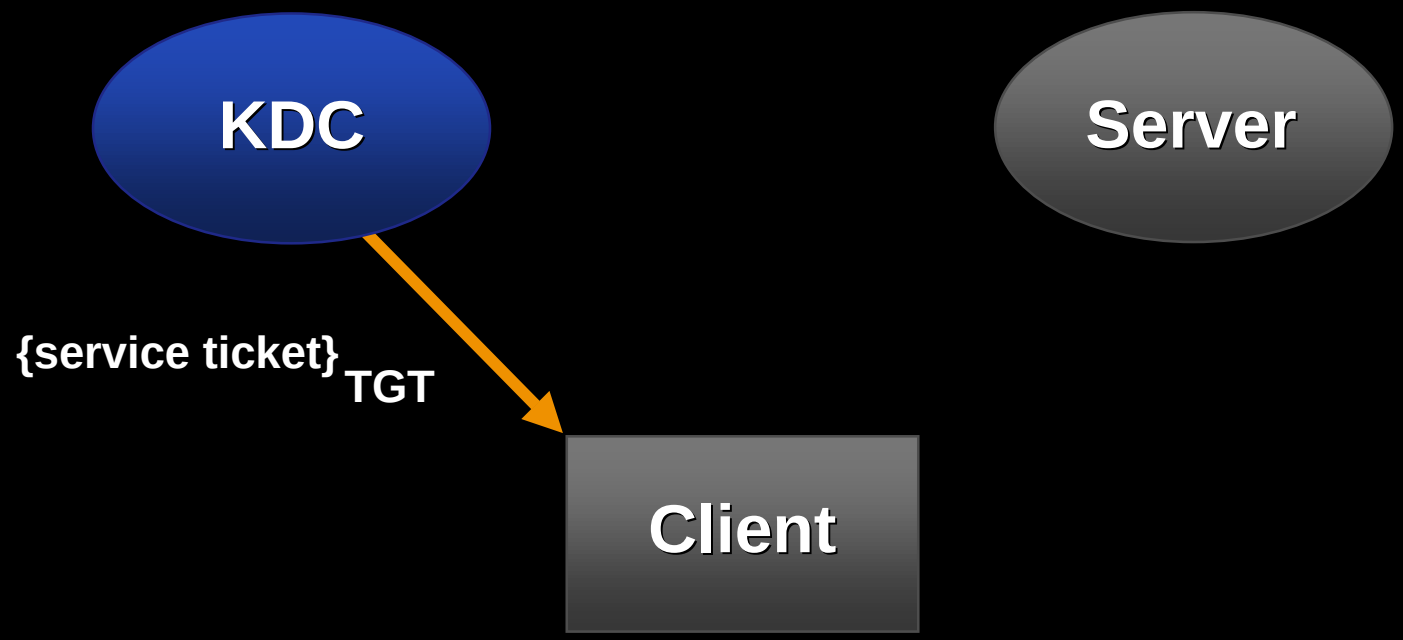
Getting a Service Ticket

- Client presents TGT to KDC with a request for a service ticket



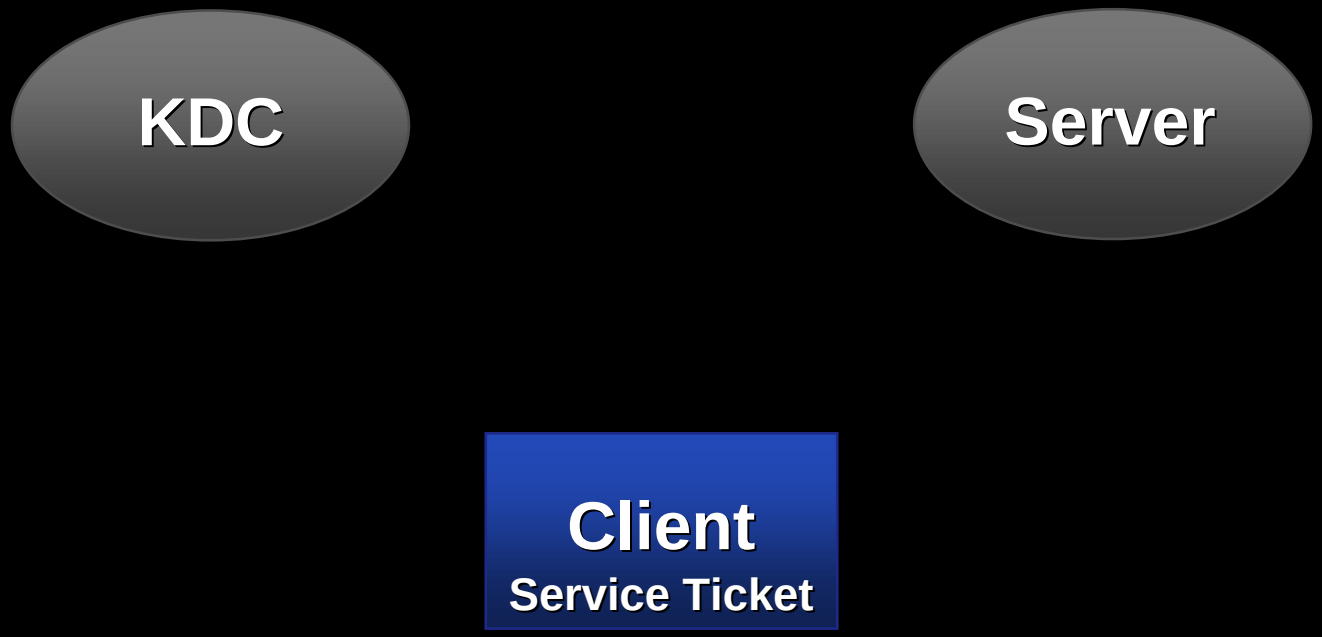
Getting a Service Ticket

- KDC returns encrypted service ticket to client



Getting a Service Ticket

- Client uses TGT to extract service ticket

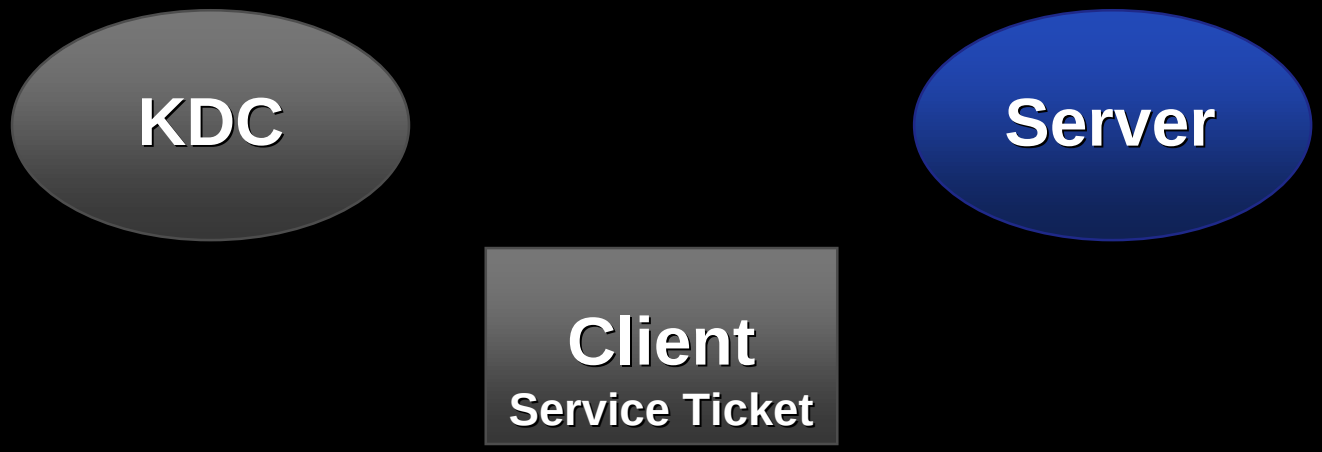


Connecting to a Service: One-Way Authentication

- Client presents service ticket to server

Connecting to a Service: One-Way Authentication

- Server receives service ticket and authenticates the client
- Server may use session key from service ticket to encrypt subsequent traffic between client and server



Connecting to a Service: Mutual Authentication

- Client sends service ticket containing session key to server

Connecting to a Service: Mutual Authentication

- Server returns a response encrypted with session key from service ticket, authenticating server to client
- Server may also use session key to encrypt subsequent traffic between client and server

Brief History of Kerberos

- Invented in the 1980's at MIT as part of Project Athena
- Protocol lineage: v4, v5
- Implementation history on the Macintosh
  - KClient, Authman, MacLeland (v4)
  - MIT/Cygnus v5
  - Kerberos for Macintosh 2.0 (slightly updated KClient and MIT v5)
  - KfM 2.5 (further updated KClient, new v5 implementation)
  - KfM 3.0 (combined v4 and v5 with single sign on)

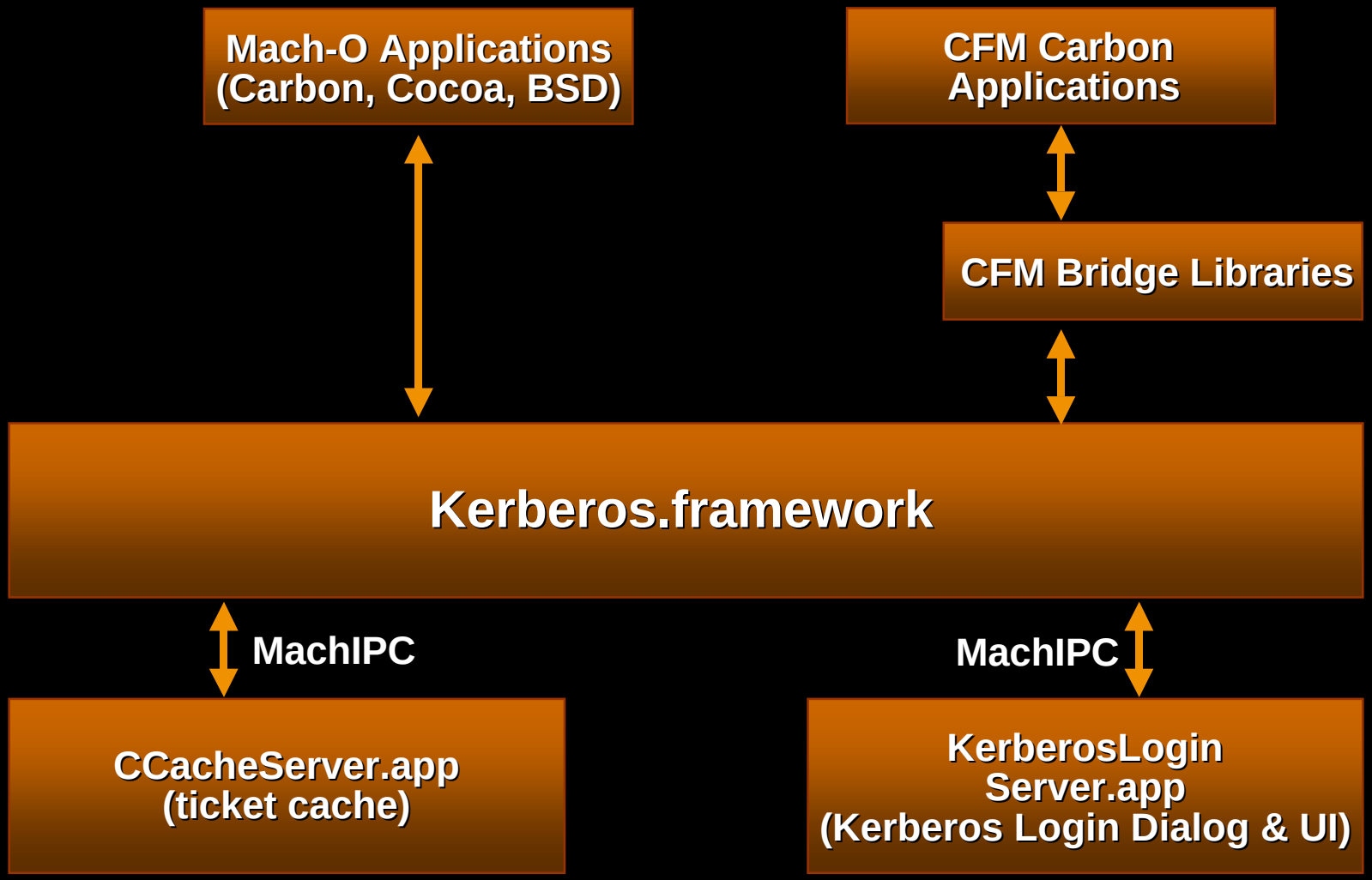
Kerberos for Macintosh 4.0

- Supports both Mac OS X and Mac OS 9
- Provides Kerberos libraries on Mac OS X to
  - Carbon
  - Cocoa
  - Command Line
- Classic Mac OS support includes
  - Mac OS 8.1 and later
  - CarbonLib 1.0.4 and later

Why Not Just Unix Kerberos?

- Does not include APIs that existing Mac applications depend on
- Does not provide functionality for the level of user interaction Mac users demand
- Does not support all runtime environments of Mac OS X

KfM 4.0 Architecture



Kerberos v4

- KClient 3.0
  - Compatibility libraries
  - New version 3 APIs
- Cygnus Kerberos v4 implementation
  - The final Cygnus release (version 96q4)
  - Modifications to support KerberosLoginLibrary
- Applications can use either API for v4 calls
  - KClient 3.0 recommended
  - Historic v4 API only for porting existing Kerberos code

Kerberos v5

- MIT Kerberos v5 1.2.2
  - Includes 3DES
  - Improved hardware preauthentication support
  - Numerous buffer overrun problems fixed
  - Partial IPv6 support
- GSS API
  - Supports RFC #1509—“Generic Security Service API : C-bindings” & RFC #1964—“The Kerberos Version 5 GSS-API Mechanism”

Credentials Cache

- Bottom layer—where the tickets/credentials are stored
- Stored in memory as opposed to on disk
- Provides API for accessing the credentials used by KClient, v4, v5 libraries

Kerberos Login Library

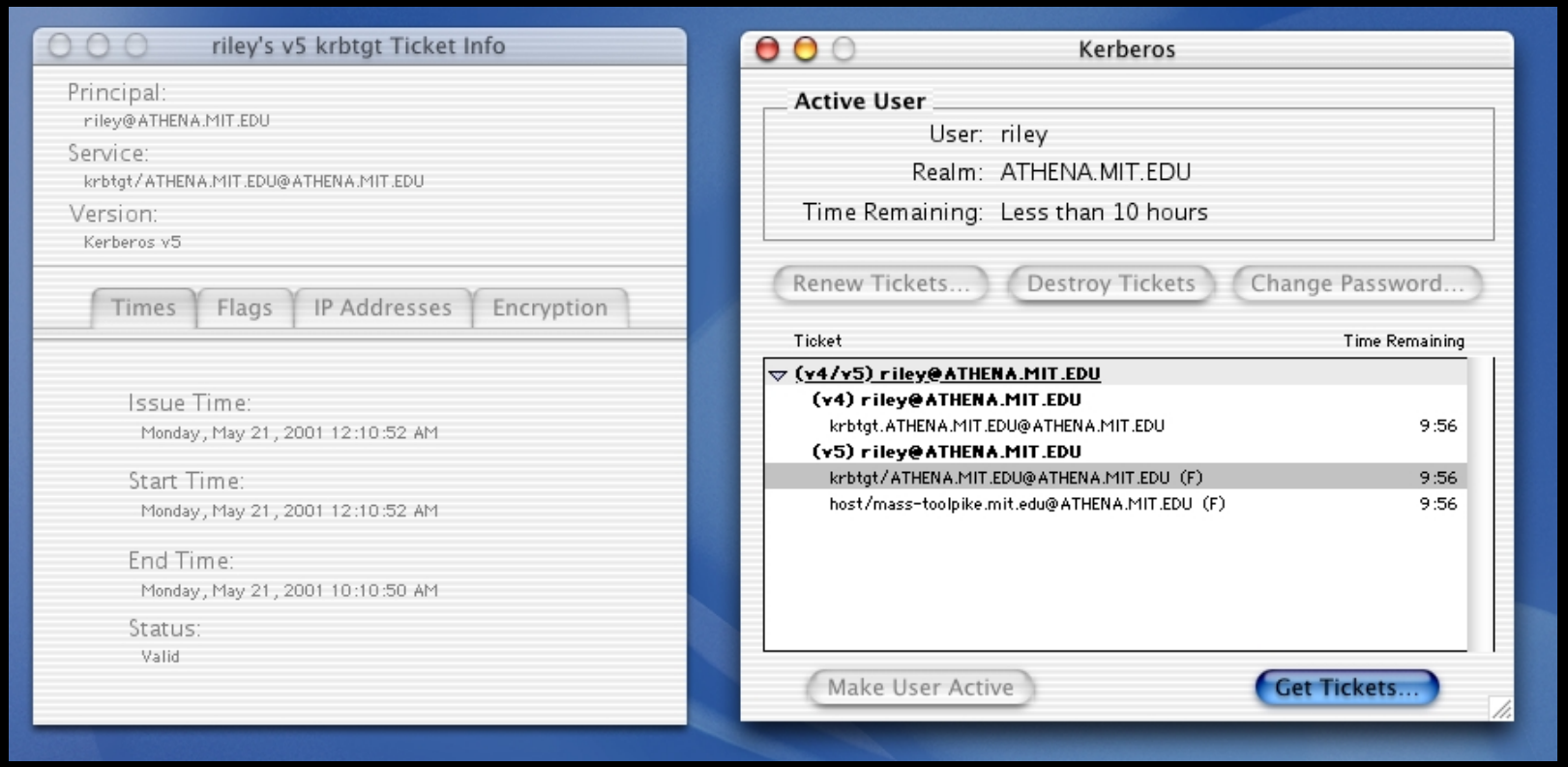
- Simplifies the process of getting Kerberos TGTs
  - Allows you to get or destroy tickets with a single call
  - Transparently handles v4 and v5 initial tickets
- Also provides API for adjusting Kerberos Login Dialog options
- Used by programs that need to perform actions on TGTs, such as administrative applications

Kerberos Login Dialog

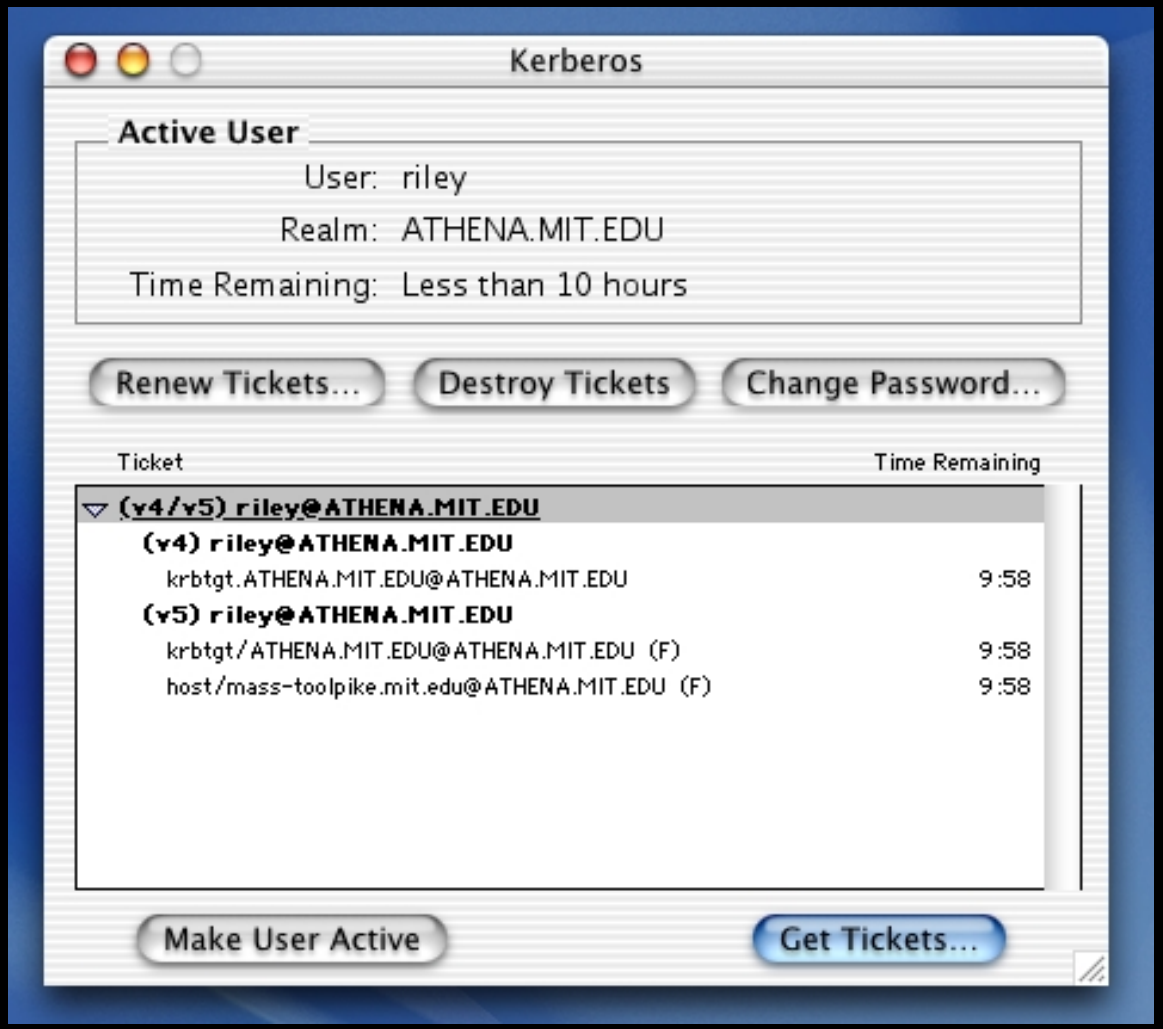
Kerberos Control Panel/Application

- Provides a UI for obtaining, destroying, listing, and displaying information about tickets and currently authenticated users
- Also provides UI for setting Kerberos Login dialog options

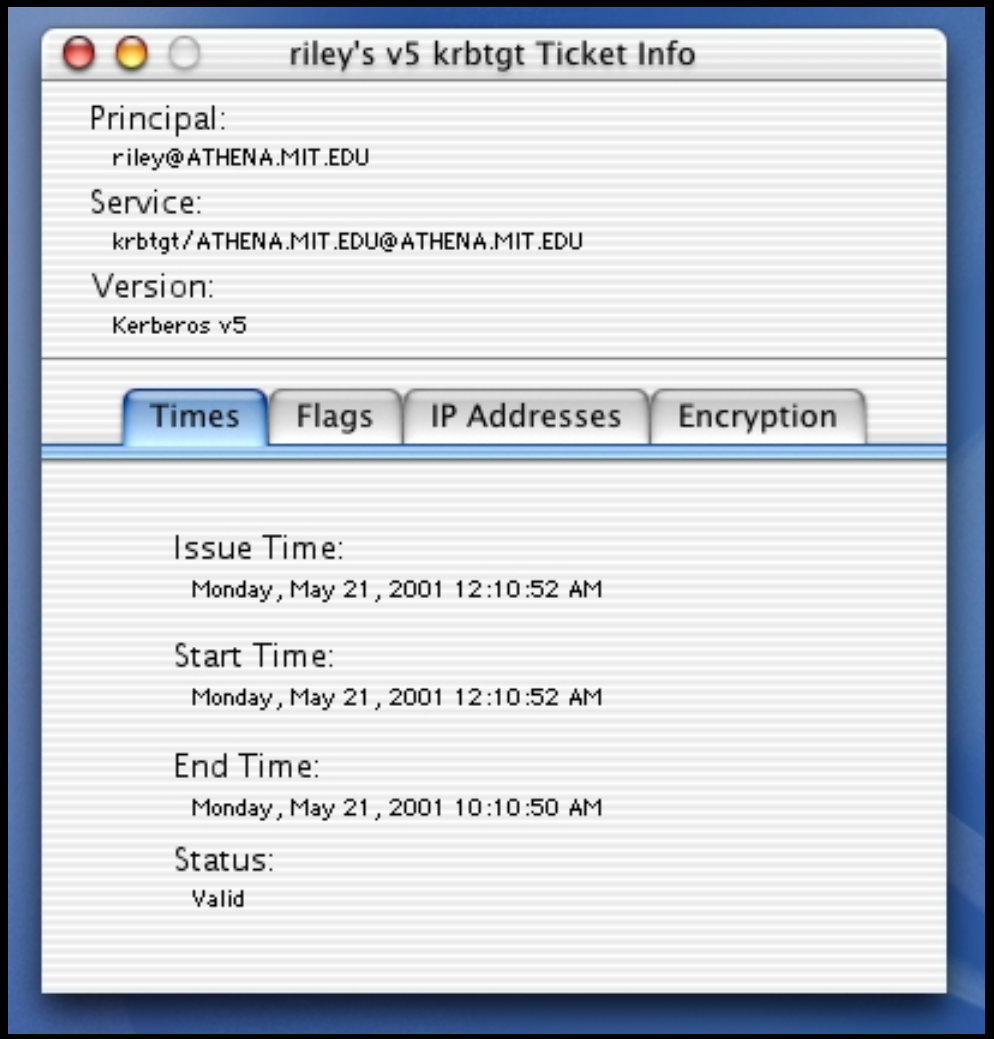
Kerberos Control Panel/Application



Kerberos Main Window



Kerberos Ticket Info Window



How to Kerberize an Application

- Find the protocol specification (RFCs, etc.)
- Determine which API to use (KClient, Kerberos v5, GSS API, etc.)
- Figure out how to connect the API to the protocol
  - The data returned by the API usually needs to be massaged into a form required by the protocol

Kerberizing FTP

- Protocol: RFC 2228, RFC 959
- Supports Kerberos v4 and GSS
  - Use KClient for Kerberos v4 (better support for multiple sessions)
  - Use GSS API for Kerberos v5

Kerberizing FTP: Kerberos v4

- Session management
  - KClientNewClientSession
- Authentication
  - KClientGetAuthenticatorForService
  - KClientVerifyProtectedServiceReply
- Encryption and decryption
  - KClientEncrypt
  - KClientDecrypt
- Connecting the API to the protocol
  - Base 64 encoding

Kerberizing FTP: GSS

- Session management and authentication
  - gss_init_sec_context
- Encryption & decryption
  - gss_wrap
  - gss_unwrap
- Connecting the API to the protocol
  - Base 64 encoding

Work in Progress

- Directory Services plug-in
  - Apple and MIT are working to define standard specification
- Login Authenticator
- More comprehensive integration

How Do I Get Started?

- Download developer release of Kerberos for Macintosh 4.0 from MIT
- Current release includes nearly all needed functionality for Mac OS X application developers
- Use on-line resources—web documentation, mailing lists and newsgroups for assistance

For More Information

- MIT Kerberos for Macintosh
  - **http://web.mit.edu/macdev/www/kerberos.html**
- Kerberos Papers and Documentation
  - **http://web.mit.edu/kerberos/www/papers.html**
- Internet RFCs
  - **http://www.ietf.org/rfc.html**
- Kerberos Development List
  - **krbdev-request@mit.edu**
- Usenet
  - **comp.protocols.kerberos**

Related Sessions

301 Mac OS X Server	Room A1 **Tues., 2:00pm**
305 Extending Security in Mac OS X: Overview of Security APIs	Room A1 **Wed., 9:00am**
306 Security: Authorization APIs	Room J2 **Wed., 10:30am**
307 Security: Keychain	Room J2 **Wed., 2:00pm**
FF113 Feedback Forum: Security	Room C **Fri., 10:30am**

Who to Contact

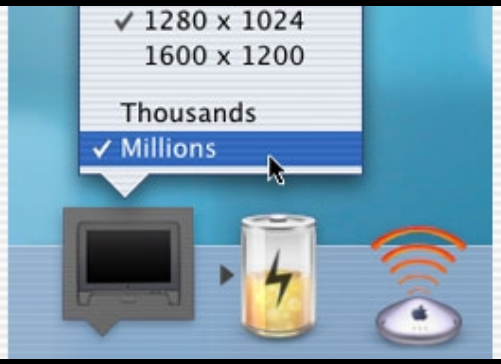
Thomas Weyer
Network & Communications Technology Manager
Apple Worldwide Developer Relations
weyer@apple.com

Marshall Vale
Project Manager: Macintosh and Kerberos Development
Massachusetts Institute of Technology
mjv@mit.edu

Craig Keithley
Security & Cryptography Technology Manager
Apple Worldwide Developer Relations
keithley@apple.com

http://developer.apple.com/events/urls.html

Q&A



Thomas Weyer
Network & Communications Technology Manager
weyer@apple.com

http://developer.apple.com/events/urls.html

WWDC
Worldwide Developers Conference 2001